El modelo europeo de protección de datos de carácter personal*

Leonardo Cervera Navas[1]
Administrador
Unidad de Protección de Datos
Dirección General del Mercado Interior
Comisión Europea

SUMARIO: La tecnología como motor principal del desarrollo del derecho a la protección de datos personales en el siglo xx.—El modelo europeo de protección de datos *versus* el modelo estadounidense.—De cómo ven los americanos el modelo europeo de protección de datos.—De la situación actual y el futuro del modelo europeo de protección de datos en la Unión Europea.

LA TECNOLOGÍA COMO MOTOR PRINCIPAL DEL DESARROLLO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL SIGLO XX

Los historiadores discrepan sobre el momento preciso en que comenzara este fenómeno que vivimos ahora tan intensamente y que se viene a denominar genéricamente con el término «globalización». Parece ser que puede hablarse de una primera globalización (europea) en tiempos del Bajo Imperio Romano, que desgraciadamente colapsó hacia el siglo v de nuestra era, y una segunda globalización (del hemisferio norte) que arranca a comienzos del siglo xix, cuando se sientan las bases del capitalismo y la economía moderna.

Hay obvias diferencias entre ambas globalizaciones, pero también increí-

---

* Artículo basado en la conferencia pronunciada en el Curso de Verano de El Escorial *Presente y futuro de la protección de datos personales,* Madrid, 19 de julio de 2004.

[1] Cuantas opiniones aparecen reflejadas en el artículo son responsabilidad únicamente del autor y no representan en modo alguno la opinión de la Comisión Europea.

bles similitudes. Hoy en día se vierten ríos de tinta sobre el proceso de aproximación de legislaciones entre los países globalizados, pero en el Imperio Romano ya se trabajaba en un Derecho de gentes (o Derecho internacional privado) que el *praetor peregrinus* hacía ejecutar en todos los rincones del Imperio Romano, sin distinción entre ciudadanos romanos y otros individuos a los que se les reconocía personalidad jurídica y capacidad de obrar.

Entre aquella primera globalización «romana» y esta segunda globalización «anglosajona» hay otras curiosas similitudes. Entonces como ahora, aquellas zonas del planeta integradas en la globalización se beneficiaron de unos niveles de vida y de lujo considerables. Los habitantes de las capitales del Bajo Imperio Romano, ya fuera en *Londinum* (Londres), *Italica* (Sevilla) y no digamos Roma, disfrutaban de importantes comodidades, agua corriente, alumbrado público, servicios públicos, etc. Entonces como ahora, aquellas zonas que no pudieron, no supieron o no quisieron beneficiarse de la globalización sufrieron altos niveles de miseria y vieron cómo la globalización no hizo sino empobrecerlos aún más. Recientes estudios demuestran que las condiciones de vida de muchos países subdesarrollados en el siglo XXI son muy similares a las de los pueblos situados fuera del *limes* del Imperio Romano.

El proceso de globalización, tanto en Roma como en nuestro tiempo, va acompañado de procesos de innovación tecnológica y reforma social. Las primeras manifestaciones espectaculares de esta globalización en la que actualmente nos encontramos inmersos se producen en el último tercio del siglo XIX, con avances tecnológicos en materia de medios de transportes y de comunicación instantánea a distancia que parecían inverosímiles a nuestros bisabuelos. El avance de la tecnología maravilla al mundo y despierta la imaginación de muchos escritores, siendo Julio VERNE uno de los más representativos. En novelas como *Un viaje a la luna* (1865) o *La vuelta al mundo en ochenta días* (1873), Julio VERNE aventura un futuro tecnológico que muy pronto va a hacerse realidad.

En la revolución tecnológica del siglo XIX se encuentra el germen de muchas de las nuevas ideas e inquietudes sociales, el nacionalismo, el socialismo, el colonialismo, etc., que son, al fin y al cabo, las responsables de que el siglo XX haya pasado a la historia como el siglo «de las guerras», pero también el siglo de una nueva sociedad, más igualitaria y respetuosa con los valores fundamentales del ser humano.

El propio Julio VERNE hacer girar su novela *20.000 leguas de viaje submarino* (1870) en torno a una invención singular (el submarino Nautilus) y un personaje tremendamente enigmático, el Capitán Nemo, un personaje sobre el que sabremos muy poco con la lectura de esta novela de peripecias submarinas, pero, afortunadamente, Julio VERNE se mostró dispuesto a desvelarnos más detalles sobre este personaje en una novela posterior, *La isla misteriosa* (1874)[2].

[2] Léase el capítulo XVI, tercera parte.

El Capitán Nemo resultó ser un príncipe hindú educado en Inglaterra «*con la secreta intención de que un día pudiese luchar, con armas iguales, contra los que él consideraba como los opresores de su país*». Por tanto, este personaje encarna la lucha contra el colonialismo y la nueva forma de explotación que ello conlleva[3], anticipando con este personaje Julio VERNE las guerras de liberación nacional que se van a suceder en Asia y África en la primera mitad del siglo XX.

Una de esas nuevas ideas e inquietudes sociales que tienen su origen directo en la revolución tecnológica es precisamente el derecho a la vida privada, *the right to privacy*. En realidad, se pueden distinguir dos momentos diferenciados en los que los avances tecnológicos motivan una reacción social en el sentido de proteger la intimidad de los ciudadanos. En un primer momento, a finales del siglo XIX, la reacción no fue mucho más allá de debates doctrinales y se circunscribió mayoritariamente a los Estados Unidos de América, mientras que en un segundo momento, tras la Segunda Guerra Mundial, la reacción social vino acompañada de desarrollos normativos a nivel nacional e internacional, con un mayor desarrollo en Europa que en los Estados Unidos.

La primera reacción, mayoritariamente americana, se relaciona con un artículo publicado por dos abogados de Boston, WARREN y BRANDEIS, en el *Harvard Law Review* en el año 1890, con el famoso título «The right to privacy». Estos abogados argumentaron, con éxito, la existencia de un derecho a la privacidad que se fundamentaba en los mismos principios del *Common Law* que sustentan derechos tradicionales tales como el derecho a la propiedad privada o el derecho a la vida. De la misma manera que el derecho a la propiedad intelectual, decían estos autores, no es más que una espiritualización del derecho a la propiedad material, el derecho a la vida se habría también extendido al derecho a *disfrutar* de la vida, el derecho *to be let alone:* el derecho a que lo dejen a uno tranquilo, que no lo fotografíen, filmen o escuchen.

En aquel primer momento, el carácter invasivo de la tecnología se manifestó en el hecho de que las crónicas de sociedad empezaban a llenarse de fotografías de personas en compañía de otras personas en eventos sociales y recepciones, y esto se consideró inaceptable y lesivo de la reputación de damas y caballeros respetables que *should be let alone*.

Si se me permite la digresión, muy recientemente (24 junio 2004), la

---

[3] «*El príncipe Dakkar odiaba. Odiaba al único país en el que nunca había querido poner el pie, a la nación de la que había rechazado ofertas y proposiciones. Odiaba a Inglaterra, tanto más cuanto que la admiraba también en más de un aspecto. (...) El científico sustituyó al guerrero. Una isla desierta del Pacífico le sirvió para establecer sus astilleros, y allí se construyó un barco submarino según sus planos. Empleó para todas las necesidades de su aparato flotante, como fuerza motriz, lumínica y calorífica, la electricidad, cuya inconmensurable fuerza mecánica supo utilizar a través de medios que algún día se conocerán, obtenida de fuentes inagotables. (…) Durante muchos años, el capitán Nemo visitó todos los océanos, de un polo a otro. Paria del universo habitado, recogió de esos mundos desconocidos admirables tesoros. Los millones perdidos en la bahía de Vigo, en 1702, por los galeones españoles, le proporcionaron una mina inagotable de riquezas, que utilizó siempre, anónimamente, en favor de los pueblos que combatían por la independencia de sus países*».

Corte Europea de Derechos Humanos se ha pronunciado sobre este aspecto de la protección de la privacidad[4] (que no de la protección de datos *strictu sensu*) y ha fallado a favor de la princesa Carolina de Mónaco, que había denunciado como contraria al artículo 8 de la Convención Europea de Derechos Humanos la aparición de determinadas fotos en una publicación alemana en las que la princesa aparecía con sus hijos en actividades completamente rutinarias, como ir de compras o pasear por el parque.

El Tribunal Europeo de Derechos Humanos ha considerado que si bien la publicación de ciertas fotografías de valor informativo puede prevalecer sobre el derecho a la intimidad de ciertas personas, sobre todo aquellas de cierta relevancia pública, el derecho a la libertad de expresión no prevalece en aquellos supuestos en los que el único interés que se percibe es el interés mercantil del tabloide, haciendo dinero con la venta de la publicación de las fotografías. Es de suponer (y esperar) que esta sentencia tendrá alguna influencia en las actividades de la denominada prensa del corazón y los fotógrafos denominados *paparazzis,* sobre todo en aquellos casos en los que la publicación de las fotografías se hace sin el consentimiento de los interesados.

Volviendo al tema que nos ocupa, es decir, cómo los avances tecnológicos han sido el principal desencadenante de la legislación en materia de protección de datos, el segundo momento en que la tecnología provoca una reacción social a favor de la protección de la intimidad se sitúa en la década de los sesenta y coincide básicamente con la aparición de las primeras computadoras (en principio sólo en manos del gobierno y de las grandes multinacionales), la proliferación de diminutos micrófonos de escucha (caso Watergate), satélites capaces de fotografiar una matrícula desde el cielo (guerra fría), etc.

En definitiva, este despliegue de tecnología, muchas veces imperceptible para los ciudadanos, aparatos que vigilan y controlan por todas partes, crea una sensación de ansiedad en la sociedad que los legisladores van a traducir unos años más tarde en las primeras legislaciones en materia de protección de datos, tanto en Europa como en los Estados Unidos (con algunas diferencias, como analizaremos más tarde).

Pero antes de que esto ocurra hay un escritor excepcional, un inglés comprometido socialmente, que luchó en las trincheras de la guerra civil española en defensa de la República y que, no obstante, no tuvo problemas en convertirse en el abanderado de la lucha contra el comunismo soviético, el visionario George ORWELL, que, con su famosísima novela *1984* (1949), enciende por primera vez las alarmas sobre los peligros de la tecnología para la privacidad de las personas.

El motor principal de *1984* no es el derecho a la intimidad, sino el miedo al totalitarismo, un totalitarismo que se presenta más abstracto que el de índole comunista de otra de sus anteriores novelas, *Animal Farm* (1945). Lo

[4] *Von Hannover v. Germany* (application no. 59320/00).

verdaderamente significativo de esta novela es que el totalitarismo inventado por ORWELL, y que éste sitúa en la Inglaterra de treinta y cinco años después, es un totalitarismo muy sofisticado que hace uso de las nuevas tecnologías para el control absoluto de la sociedad. Mediante el uso del *telescreen* (una especie de televisión interactiva muy similar a Internet) y micrófonos ocultos por toda la ciudad, el Gran Hermano lo ve y lo escucha todo, y el protagonista, que se atreve a dudar de las mentiras que diariamente inundan los periódicos, acaba sucumbiendo tras la tortura al *doublethinking*, es decir, la posibilidad de darse uno cuenta de que la noticia del partido tiene la apariencia de falsa pero, al mismo tiempo, creerla sin mayor reflexión.

En puridad, *1984* alerta a la sociedad europea y americana de posguerra del peligro cierto de que la tecnología, la cual se percibe normalmente como orientada hacia la moral, puede convertirse en el más peligroso aliado del totalitarismo.

En 1984, el mundo no sucumbió al totalitarismo del Gran Hermano de la novela, pero pasaron algunas cosas interesantes. Por ejemplo, Chernenko sustituyó a Andropov a la cabeza de la Unión Soviética. Las Olimpiadas de Invierno de Sarajevo se celebraron con gran éxito, que los rusos empañaron en parte al anunciar el boicot a las próximas Olimpiadas en Los Ángeles. Doce personas murieron en un ataque suicida a la embajada estadounidense en Beirut. Gerry Adams y Margaret Thatcher sobrevivieron milagrosamente a sendos atentados terroristas. Indira Gandhi ordenó un ataque contra el «Templo Dorado», lugar sagrado de los Sikh, y murió asesinada poco después en el jardín de su residencia por dos de sus guardaespaldas Sikh. Dos mil Sikh inocentes murieron en los días siguientes en altercados callejeros. Tres mil ochocientas personas murieron en el desastre de Bhopal, cuando un escape en una planta de pesticidas en la India envenenó a medio millón de personas mientras dormían. Por último, Apple lanzó al mercado el primer ordenador doméstico con ratón y anunció un nuevo invento para 1985: el ordenador portátil.

Personalmente, creo que los miedos de George ORWELL hacia la tecnología estaban bien justificados. Un libro publicado en el año 2001[5] profundiza en las relaciones comerciales entre la multinacional IBM y el Tercer Reich y demuestra cómo las autoridades nazis no hubieran sido jamás capaces de llevar a cabo sus políticas raciales sin la ayuda de pre-computadoras fabricadas por una filial alemana de la compañía estadounidense IBM[6]. Estas máquinas tabuladoras, que funcionaban con fichas perforadas, fueron vitales para la elaboración del censo alemán de 1937 (identificado en el juicio de Nuremberg como uno de los primeros pasos del holocausto judío) y habrían permitido al régimen nazi realizar búsquedas cruzadas de apellidos, familias y patrimonios.

---

[5] *IBM and the Holocaust,* by Edwin Black, Little Brown.

[6] La compañía IBM ha negado públicamente cualquier responsabilidad y mantiene que la filial alemana fue tomada por los nazis desde el primer momento, por lo que perdieron cualquier control desde Estados Unidos. Hay voces discrepantes al respecto.

En particular, según se indica en este libro, fue sólo tras la introducción de un nuevo modelo de máquina tabuladora que incluía «una ficha suplementaria» que fue posible rastrear los antecedentes raciales de toda la población del Reich (80 millones de personas) e identificar a los que se denominó «judíos raciales» (330.530 personas), que posteriormente la máquina subdividió en «judíos totales» y otras categorías de «judíos parciales», conteniendo cada ficha la dirección de cada uno de estos judíos, a los que, lógicamente, se fue a buscar llegado el momento oportuno para su traslado a «campos de trabajo».

Así pues, y concluyendo este repaso histórico y literario, las experiencias totalitarias de pre-guerra y los avances de la tecnología, sobre todo en materia de computadoras, se aliaron finalmente para que, en primer lugar, el artículo 8 de la Convención Europea de Derechos Humanos reconociera el derecho al respeto a la vida privada y familiar, casa y correspondiera (antecedente directo de la protección de datos) y, seguidamente, se produjera un intenso debate sociológico y después político en las décadas de los sesenta y setenta en Europa y Estados Unidos, que, sobre todo con la irrupción masiva de los ordenadores, culminó en desarrollos legislativos en materia de protección de datos en la década de los ochenta. Estos desarrollos legislativos se produjeron a nivel nacional tanto en Europa como en los Estados Unidos, y a nivel regional europeo con la Convención 108 del Consejo de Europa, sobre la protección de las personas en relación al tratamiento automatizado de datos personales. El derecho a la protección de datos, en su configuración más clásica en el sentido del artículo 8 de la Convención Europea de Derechos Humanos, se incorporó también a muchas de las Constituciones de los Estados europeos.

Este proceso normativo europeo culminó en la década de los noventa con la aprobación, el 28 de octubre de 1995, de la Directiva europea de protección de datos, el marco legislativo horizontal sobre protección de datos más avanzado del mundo hasta la fecha, el cual ha sido completado con posterioridad por la Directiva sobre privacidad en las telecomunicaciones (2002/58/CE) y el Reglamento 2001/45/CE, que aplica la normativa europea a las propias instituciones comunitarias.

Finalmente, y como colofón importantísimo, el Proyecto de Constitución para Europa recoge un artículo sobre protección de datos, de tal forma que cuando el proceso de ratificación finalice en noviembre del 2006 (esperemos que felizmente) y la Constitución europea entre en vigor, el derecho a la protección de datos estará finalmente reconocido como un derecho fundamental de la Unión Europea, inmediatamente detrás del derecho al respeto a la vida privada y familiar, inviolabilidad del domicilio y correspondencia, e inmediatamente antes que el derecho a casarse y fundar una familia. Habrá sido éste el final de un largo camino en el que algunas personas han tenido un protagonismo muy particular, alguna de ellas ponente en este seminario, como el Profesor Stefano RODOTÀ, que me ha precedido en el uso de la palabra, defensor y promotor de la *privacy* en Italia y en la esfera internacional

desde la década de los setenta y uno de los participantes en la elaboración de la Carta Europea de Derechos Fundamentales del año 2000, antecedente inmediato del capítulo de derechos fundamentales contenido en el Proyecto de Constitución para Europa.

EL MODELO EUROPEO DE PROTECCIÓN DE DATOS *VERSUS* EL MODELO ESTADOUNIDENSE

Hemos visto con anterioridad que Estados Unidos fue pionero en las discusiones sobre privacidad. Estados Unidos tiene una larga tradición democrática y de protección de los derechos y libertades del individuo y estuvo a la cabeza de las innovaciones tecnológicas que fueron el motor de este debate sobre la protección de datos; por tanto, no es casualidad que se percibiera el problema ya en 1880 por un par de abogados de Boston. En la actualidad, sin embargo, el sistema de protección de datos estadounidense está muy lejos de los estándares europeos. Esto parece paradójico: ¿por qué el legislador americano se ha quedado atrás o por qué el legislador europeo ha podido avanzar más que el americano?

La respuesta a esta pregunta no es fácil, ya que parecen haberse combinado una serie de factores sobre cuya influencia exacta no podemos más que especular. Uno de los autores que más parece haber profundizado en estas cuestiones es Priscila M. REGAN. Algunas de las ideas expresadas a continuación aparecen recogidas en su libro de 1995 que lleva el significativo título de *Legislating Privacy*[7].

La primera razón de este atraso estadounidense en materia de protección de datos parece ser la propia configuración del *Common Law* y la definición que el derecho a la protección de datos ha recibido históricamente en la jurisprudencia y en la doctrina estadounidenses.

En primer lugar, la Constitución estadounidense no contiene referencia alguna a la privacidad y ninguna de sus enmiendas posteriores está directamente relacionada con este derecho. La primera consecuencia de esta ausencia en la Constitución es que la existencia de este derecho (como hicieran WARREN y BRANDEIS en 1890) tiene que extraerse de otros principios del *Common Law*, lo cual ha supuesto cierta indefinición sobre el contenido de este derecho y ha restado fuerza a cuantas propuestas legislativas se han presentado.

Mientras que en Europa el respeto a la vida privada aparece claramente recogido en la Convención Europea de Derechos Humanos y en algunas Constituciones nacionales, en los Estados Unidos de América, por el contrario, durante mucho tiempo se especula sobre qué es este derecho *to be left alone* que se desprende del *Common Law*. Se da, además, la circunstancia de

[7] Priscila M. REGAN, *Legislating Privacy. Technology, social values and public policy*, Chapel Hill, 1995.

que este *derecho a que lo dejen a uno tranquilo* parece entrar en contradicción con uno de los sacrosantos principios del Derecho constitucional americano: el derecho a la libertad de expresión, reconocido en la primera enmienda constitucional. Esto no ayuda al desarrollo de este derecho.

En segundo lugar, el derecho a la protección de datos no se considera un *civil right*. En la tradición legal estadounidense se diferencian dos grandes categorías de derechos: los derechos civiles *(civil rights)* y las libertades públicas *(civil liberties).* El derecho a la protección de datos, que debería haberse caracterizado como un *civil right* en su origen, se presenta en realidad como una *civil liberty,* que además sería de naturaleza negativa: *the right to be left alone*. Las libertades públicas ceden más fácilmente frente a otros intereses que los derechos civiles.

Al mismo tiempo, al tratarse de un derecho cuyo desarrollo va directamente ligado al desarrollo de la tecnología, en un país como los Estados Unidos, donde los grupos empresariales han tenido tradicionalmente gran influencia sobre el poder legislativo, aquellos que se benefician de los progresos tecnológicos van a ejercer su influencia para evitar que la protección de datos pueda eventualmente constituirse en un obstáculo al progreso de esa tecnología que promete tan pingües beneficios. A esta considerable influencia empresarial parece haberse aliado el hecho de que, en los Estados Unidos de América, el tema de la privacidad no parece arrastrar muchos votos y, en consecuencia, pocos políticos relevantes han hecho de la legislación en esta materia su bandera política.

Todo esto, conjunta y separadamente, puede explicar por qué los progresos en materia de protección de datos en Estados Unidos han sido tan escasos hasta la fecha y por qué las previsiones para el futuro inmediato en este sentido no son demasiado optimistas. A cuanto se ha señalado con anterioridad han venido a añadirse recientemente un par de factores adicionales que también actúan como freno de posibles desarrollos legislativos en materia de protección de datos en los Estados Unidos:

a) el hecho de que la población estadounidense se ha ido acostumbrando paulatinamente a la presencia de una tecnología que ya no percibe como tan peligrosa, del punto y hora de que ha entrado en sus hogares (véase la domótica, Internet o los ordenadores personales);
b) el miedo a los atentados terroristas hace que la población se muestre más proclive a aceptar que esa libertad negativa que es su derecho a la privacidad se vea limitada por otros intereses que la superan, como son la defensa y la seguridad.

Por consiguiente, el enfoque horizontal o declarativo general que existe en Europa sobre la protección de datos no existe en los Estados Unidos, un país que hasta la fecha se ha limitado a legislar en materia de protección de datos podríamos decir que *a la defensiva*, es decir, de manera sectorial, para cubrir necesidades concretas y como respuesta a un asunto que haya calado

en la opinión pública norteamericana y sobre el que se haya constatado una necesidad social importante.

Ése fue el caso de la *Video Privacy Protection Act of 1998*, una Ley aprobada un año después de que se provocara un gran escándalo en la opinión pública cuando un periódico de Washington, después de acceder a los archivos computerizados de un establecimiento de alquiler de películas de vídeo, publicara los títulos de las películas que había alquilado Robert Bork, candidato al Tribunal Supremo estadounidense. Como consecuencia de este escándalo, la Ley de 1998 prohíbe a estos establecimientos desvelar los nombres de sus clientes y las películas alquiladas.

Además de cuanto se ha señalado hasta ahora, como reiteradamente señala en su libro la Sra. REGAN, el verdadero problema para el desarrollo de la protección de datos en los Estados Unidos de América ha sido el hecho de que la *privacy* se haya examinado siempre desde una óptica liberal, es decir, como un asunto del individuo frente al Estado (o del individuo contra las corporaciones empresariales que procesan datos en contraposición al individuo). Este enfoque es incompleto pues responde sólo a una parte del problema, es decir, a la posibilidad que el individuo tiene de reaccionar contra aquellos que intentan atentar contra su intimidad. Sin embargo, el enfoque europeo es mucho más completo y abarca una dimensión social: con independencia de que el tratamiento pueda o no afectar al individuo, el Estado (o las corporaciones empresariales) tiene prohibido tratar los datos en una manera contraria a la ley o a los derechos fundamentales del individuo.

Ésta es la gran diferencia entre el enfoque europeo, en su configuración como derecho fundamental, y el enfoque estadounidense (o anglosajón), de base puramente liberal. Existe, sin embargo, una forma de tender un puente entre estas dos concepciones, como trataré de demostrar al final de esta disertación, y ese puente no es otro que la autorregulación.

DE CÓMO VEN LOS AMERICANOS EL MODELO EUROPEO DE PROTECCIÓN DE DATOS

Antes de entrar en reflexiones sobre cómo aproximar ambos modelos, el europeo y el estadounidense, me interesa hacer un ejercicio de autocrítica sobre el modelo europeo, dando la palabra a aquellos que consideran que nuestro modelo europeo de protección de datos no es el mejor de los posibles. A este lado del Atlántico es frecuente encontrar reflexiones sobre las bondades del sistema europeo de protección de datos y los defectos del sistema estadounidense de protección de datos, pero reflexiones al contrario no son tan frecuentes. Quizá se hace preciso meditar sobre lo que «los otros» piensan de nuestro modelo de protección de datos como un derecho fundamental para comprender verdaderamente las características del modelo europeo.

De cuantos artículos críticos se han publicado con el sistema europeo de

protección de datos, creo que hay uno que, por particularmente agresivo o provocador, se ha hecho famoso entre los especialistas de protección de datos, al menos entre los que trabajamos en Bruselas. Se trata del artículo publicado por Lucas BERGKAMP, abogado de la firma estadounidense Hunton & Williams, y que lleva por (revelador) título «¿Es la política europea de protección de datos adecuada para la sociedad de la información?»[8].

La conclusión de este autor es negativa, es decir, que el modelo europeo está anticuado y que la concepción europea de protección de datos, en lugar de servir a los intereses del ciudadano, acabará por perjudicarle seriamente, en base a una serie de motivos que resumidamente expongo a continuación.

El Sr. BERGKAMP cuestiona algunos de los pilares sobre los que se fundamenta el modelo europeo de protección de datos personales, empezando por su configuración como derecho fundamental del individuo. Este autor cree que el derecho a la protección de datos no puede ser un derecho fundamental porque esto significaría que al derecho a la privacidad no se puede renunciar, algo que este autor considera paradójico: si alguien quiere renunciar a su privacidad a cambio de conseguir servicios más baratos, ¿por qué impedírselo? (autonomía de la voluntad de las partes). En opinión de este autor, con la excusa de hacer a los consumidores más libres, se les hace esclavos de unos estándares de protección de la intimidad que muchos estarían dispuestos a renunciar con tal de conseguir productos más baratos.

El principal problema radicaría, en opinión de este autor, en que el modelo europeo se basa en la suposición inconfesada de que el capitalismo salvaje y sin control constituye un riesgo para la intimidad de las personas y puede provocar serios daños a los ciudadanos. Esto explica que el trabajo que se asigna a las agencias nacionales de protección de datos sea excesivamente paternalista.

En realidad, nos dice el Sr. BERGKAMP, la verdadera cuestión está en si debemos dejar al mercado o a los gobiernos regular el nivel de privacidad[9]. La respuesta que encuentra este autor a esta pregunta fundamental es la respuesta que hasta la fecha viene proponiendo el sistema americano: la intervención del legislador en materia de protección de datos debe responder a fallos concretos del sistema, siendo incorrecto que el legislador intervenga con carácter general sobre el nivel de privacidad en todos los mercados, ya que el remedio puede ser peor que la enfermedad.

Concluye el autor, por lo tanto, que el debate sobre las bondades o defectos del sistema europeo debe realizarse sobre la base de datos informados, no riesgos hipotéticos a la intimidad; sobre daños reales, no daños posibles. En definitiva, la tesis del autor es que la legislación se pronuncie únicamente sobre aquellos tratamientos de daños personales que son dañinos para las

---

[8] «Is Europe's Data Protection Policy Suitable for the Information Society?». Copyright 2001. Hunton & Williams.

[9] «*The privacy issue presents a classical choice of political philosophy: do we rely on the market or on the government to produce and deliver privacy? Who do we trust to resolve our privacy issues: technology companies or governments?*».

personas y, en su caso, su indemnización, pero se descarte, de una vez y para siempre, una aproximación general de leyes de privacidad para todos y en todas las circunstancias.

Las opiniones del Sr. BERGKAMP son respetables pero poco convincentes. Las mismas razones que éste utiliza para argumentar que el modelo europeo de protección de datos es inviable, *a sensu contrario,* servirían para argumentar que el modelo estadounidense de protección de datos no sirve para lo que se supone de un modelo de protección de datos, es decir, para proteger la privacidad de las personas.

Así, en la misma línea de ideas presentada por el Sr. BERGKAMP pero *a sensu contrario,* el modelo americano se basaría en la suposición inconfesada de que la intervención del legislador sobre la economía es perniciosa y que hay que dejar a los mercados que se autorregulen por sí solos. Sin embargo, y como creemos haber demostrado en nuestra introducción histórica, no hay garantías de que los mercados apuesten por una aproximación ética o moral al desarrollo de las tecnologías.

En resumen, las argumentaciones del Sr. BERGKAMP no demuestran que el modelo europeo de protección de datos sea inviable, pero sí evidencian muy a las claras que el modelo europeo de protección de datos, presentado como derecho fundamental del individuo, inalienable y anclado en consideraciones de justicia social, es incómodo para los que se sitúan en posiciones puramente liberales. Para éstos, el modelo estadounidense presentaría mayores ventajas.

DE LA SITUACIÓN ACTUAL Y EL FUTURO DEL MODELO EUROPEO DE PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA

En pocas palabras, la situación de la protección de datos en la Unión Europea no puede calificarse como mala, pero pocos dudarían en calificarla como mejorable.

Aquellos que, como el Sr. BERGKAMP, tratan de poner en cuestión los principios del modelo europeo de protección de datos gozan de muy poco respaldo en Europa. Estos principios parecen sólidos y gozan del apoyo mayoritario de la población europea y de sus representantes políticos. Así lo demuestran, por ejemplo, los resultados del Eurobarómetro sobre la situación de la protección de datos en la Unión Europea, realizado a finales del año 2003[10]: el 60% de los ciudadanos está preocupado por el tema de la protección de la intimidad (mucho o razonablemente), mientras que sólo el 13% de la población dice no estar preocupado en absoluto por el tema.

Por el contrario, aquellos que, desde el respeto a los principios de protección del modelo europeo, piden mejoras en su aplicación práctica por parte de los Estados miembros gozarían de mayores simpatías. Así, tendrían mu-

[10] *http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_highlights.pdf*

cha razón los que piden que se hagan esfuerzos para reducir las diferencias entre las legislaciones de protección de datos de los Estados miembros de la Unión Europea, ya que discrepancias sobre cómo debe transponerse a Derecho interno tal o cual artículo de la Directiva de protección de datos en España, Francia o Portugal, en nada benefician a la protección de la intimidad de los ciudadanos, pero sí ocasionan considerables dificultades y costes añadidos para las empresas que operan a nivel europeo.

Llevarían también bastante razón los que piden que las autoridades de protección de datos renueven sus esfuerzos para sancionar a aquellas empresas y Administraciones públicas que incumplen las normas, sobre todo aquellas relativas a la prohibición de transferir datos personales a países que no ofrecen un nivel de protección adecuado.

En fin, llevarían mucha razón los que denuncian que la protección de datos y la existencia de autoridades nacionales de supervisión son todavía desconocidas para la mayoría de la población[11]. Si la gente desconoce la existencia de sus derechos y si las autoridades de control raramente sancionan incumplimientos, es muy difícil que las empresas y las Administraciones públicas se sientan compelidas a cumplir con la legislación sobre protección de datos, y esto es muy preocupante.

Para los próximos años, por tanto, el desafío no se encuentra en reescribir el derecho a la protección de datos, sino en su redescubrimiento, de tal forma que ciudadanos y responsables del tratamiento sepan y ejerciten sus derechos y obligaciones, con los beneficios que de tal cumplimiento de la legislación se derivarán para la sociedad en su conjunto.

Queda, por supuesto, pendiente la cuestión de cómo va a ser posible reconciliar el modelo europeo de protección de datos con otros modelos extranjeros, tal como el estadounidense. No parece fácil que el Congreso de los Estados Unidos vaya a aprobar una legislación similar a la europea en un futuro próximo, ni tampoco parece probable que los países europeos vayan a secundar los estándares de protección y el enfoque minimalista del sistema estadounidense. Los tiempos en los que la respuesta a este tipo de situaciones de conflicto era la adopción de medidas proteccionistas y el cierre de los mercados forman ya parte de la historia. En la actualidad, siendo imposible igualar las legislaciones, la tendencia paulatina es hacia la convergencia de las mismas.

Básicamente, existen dos modelos de convergencia que no son incompatibles, sino, antes al contrario, compatibles y simultáneos. A la espera de un acuerdo internacional sobre protección de datos personales, al estilo de la Convención del Consejo de Europa número 108[12], es preciso avanzar por la senda de la autorregulación de las empresas establecidas en terceros países

[11] El 68% de los ciudadanos entrevistados en el Eurobarómetro del año 2003 no había oído hablar de la existencia de autoridades nacionales de protección de datos, y el 61% desconocía la existencia de legislaciones nacionales que otorgan a los ciudadanos el derecho a acceder a sus propios datos personales y a tener estos datos corregidos en caso de que fueran incorrectos.

[12] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm*

bajo la supervisión de las autoridades de control de esos países o, en su defecto, de las autoridades europeas de control.

El acuerdo de Safe Harbor entre la Unión Europea y los Estados Unidos de América del año 2000[13] es un buen ejemplo de esta autorregulación controlada, pero no es el único. Escenarios de códigos de conducta aplicados internacionalmente por las empresas bajo la supervisión de las autoridades europeas de protección de datos constituyen también un horizonte cercano muy esperanzador.

En realidad, se trata de que las empresas estadounidenses que quieren procesar datos de ciudadanos europeos asuman los principios básicos del modelo europeo y comprendan que, para los europeos, la protección de datos y la intervención de las autoridades públicas empiezan desde el momento en que una empresa decide recoger datos personales de los ciudadanos y crear una base de datos con los mismos, y no cuando esa base de datos empieza a crear problemas a los consumidores o se hace preciso sancionar. Para convencer a las empresas estadounidenses de la necesidad de este autocontrol habrá que combinar la persuasión, haciendo las cosas tan fáciles como sea posible, con la disuasión, sancionando a aquellos que, disponiendo de los medios humanos y económicos para hacer las cosas como es debido, no lo hicieren, poniendo por tanto en grave en peligro la privacidad de ciudadanos europeos.

Pretender que una empresa estadounidense cambiará, de la noche a la mañana, su filosofía de empresa y su modelo empresarial, tan sólo porque existe una ley de protección de datos en un país europeo en el que opera (entre otros muchos países alrededor del mundo), no es realista. El fenómeno de la autorregulación llevará algún tiempo. Desesperarse y renunciar a todo control sobre transferencias internacionales, con el argumento de que la empresa responsable se encuentra fuera de la jurisdicción europea y nada puede hacerse, no es una opción tampoco.

Por lo tanto, el desafío para la protección de datos en los próximos años tiene una doble naturaleza:

a) interna, disminuyendo las diferencias entre legislaciones nacionales europeas al mínimo, con el debido respeto a las particularidades de la legislación y cultura nacionales, asegurando que las normas se cumplen y se hacen cumplir con igual rigor en toda la UE, y
b) externa, buscando la convergencia con otros modelos e intentando que otras regiones del planeta se unan a nuestros esfuerzos por la defensa de un derecho fundamental del individuo.

[13] *http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2002-196/sec-2002-196_es.pdf*